INTRODUCTION À LA SÉCURITÉ INFORMATIQUE

ANTOINE TOHMÉ

PLAN

I. QU'EST CE QU'UN SYSTÈME D'INFORMATION
II. INTRODUCTION À LA SÉCURITÉ INFORMATIQUE
III. OBJECTIFS DE LA SÉCURITÉ INFORMATIQUE
IV. TERMINOLOGIE DE LA SÉCURITÉ INFORMATIQUE
V. LES MENACES LES PLUS COURANTES
VI. PIRATES (HACKERS)
VII. ÉTUDES DES CAS
VIII. CONSEILS POUR PROTÉGER VOTRE ORDINATEUR



I- QU'EST CE QU'UN SYSTÈME D'INFORMATION



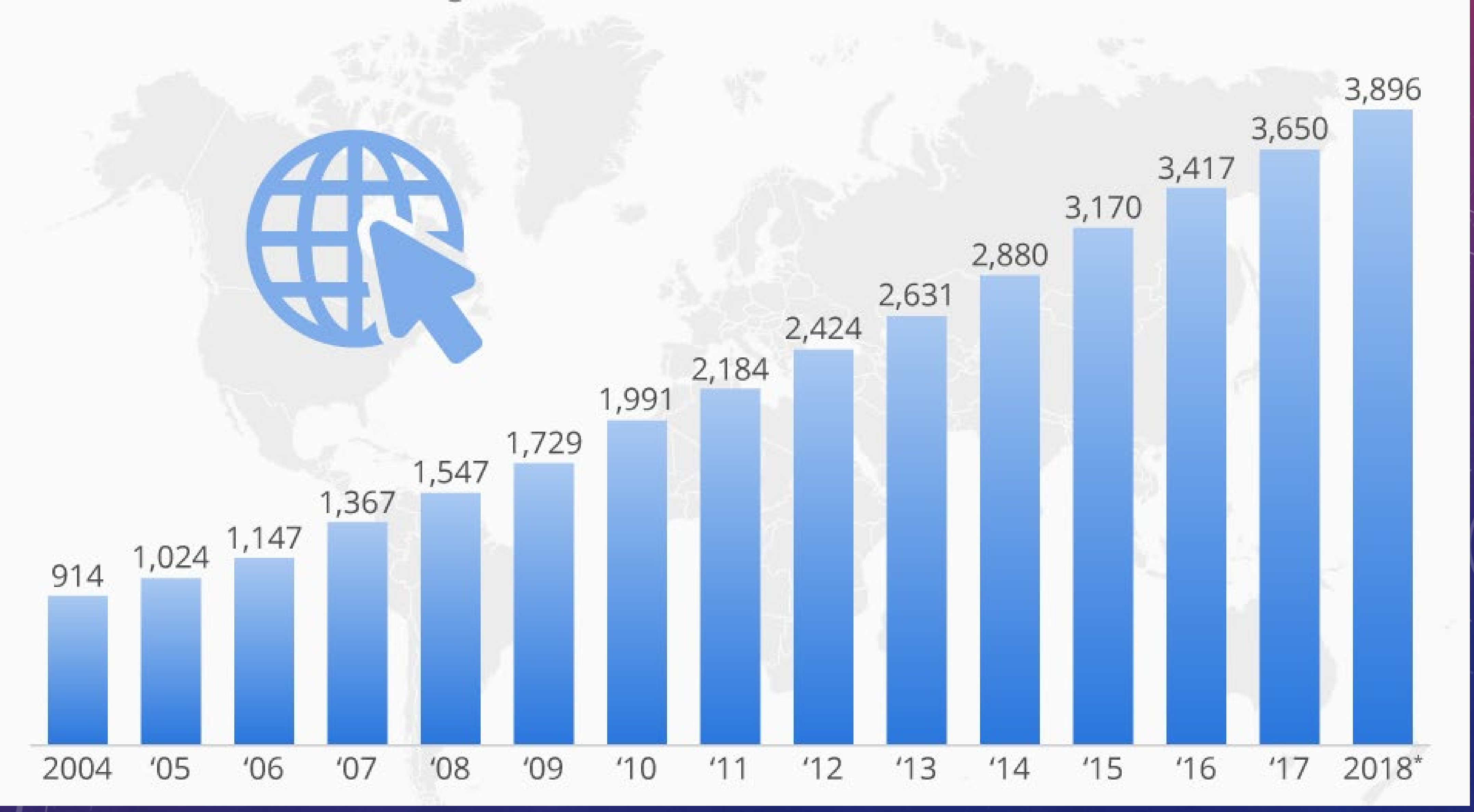
- Le système d'information est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un ordinateur, une tablette, un téléphone, etc…

- Il est composé de:
  - ✓ Utilisateurs: Personnes individuelles ou des entreprises.
  - ✓ Informatique: Matériel, logiciels et équipements de télécommunication.



II- INTRODUCTION À LA SÉCURITÉ INFORMATIQUE

- En 1988 et avant, l’internet n’était pas comme celui de nos jours.
- Il y avait environ **60 000 ordinateurs** au total dans le monde.
- La plupart des utilisateurs était des gens honnêtes, de ce fait les failles de sécurité étaient ignorées.
- Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs.
- Il est donc essentiel de connaître les ressources à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.



Half of the World Will Be on the Worldwide Web
Number of individuals using the internet between 2004–2018 (in millions)
914
1,024
1,147
1,367
1,547
1,729
1,991
2,184
2,424
2,631
2,880
3,170
3,417
3,650
3,896
2004
'05
'06
'07
'08
'09
'10
'11
'12
'13
'14
'15
'16
'17
2018*


2019 This Is What Happens In An Internet Minute
facebook
1 Million Logging In
18.1 Million Texts Sent
YouTube
4.5 Million Videos Viewed
Google play
App Store
390,030 Apps Downloaded
347,222 Scrolling Instagram
87,500 People Tweeting
1.4 Million Swipes
tinder
188 Million Emails Sent
1 Million Views
twitch
41 Music Streaming Subscriptions
180 Smart Speakers Shipped
amazon echo
Google Home
GIPHY
4.8 Million Gifs Served
41.6 Million Messages Sent
Facebook Messenger
WhatsApp
2.1 Million Snaps Created
$996,956 Spent Online
NETFLIX
694,444 Hours Watched
Google
3.8 Million Search Queries
60 SECONDS
Created By:
@LoriLewis
@OfficiallyChadd

III- OBJECTIFS DE LA SÉCURITÉ INFORMATIQUE

Confidentialité

Disponibilité

Intégrité

Authentification

1- CONFIDENTIALITÉ DE L'INFORMATION

Garantir que l'accès à l'information et aux données n'est autorisé que pour les personnes autorisées à les consulter.



2- DISPONIBILITÉ DE L'INFORMATION

Garantir que la ressource ou l'information sera disponible à tout moment, ou a minima accessible quand une personne souhaitera l'utiliser.



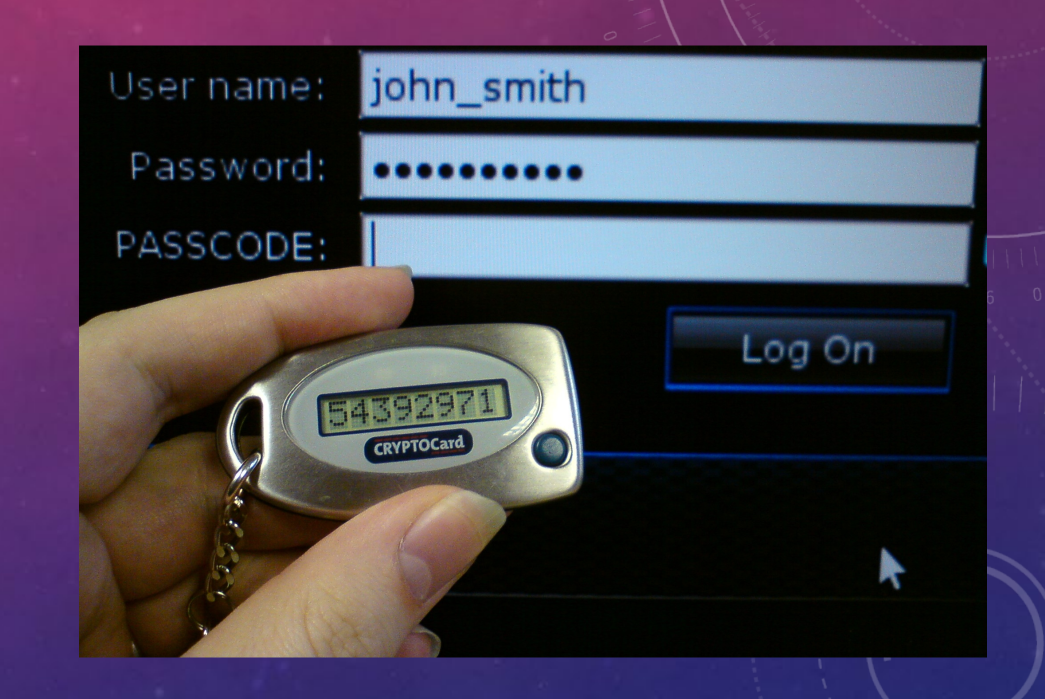
3- INTÉGRITÉ DE L'INFORMATION

Garantir que les données ou informations stockées ne soient pas modifiées par un tiers, c'est-à-dire quelles conservent leur pertinence et empêchant une altération de celle-ci.



4- AUTHENTIFICATION

Vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel.



IV- TERMINOLOGIE DE LA SÉCURITÉ INFORMATIQUE

Vulnérabilité

Menace

Attaque

1- LES VULNÉRABILITÉS

- Ce sont les failles de sécurité dans un ou plusieurs systèmes.

- L'exploitation d'une vulnérabilité pourrait permettre à un attaquant (ex. Hacker) ou un programme malveillant de réaliser des actions malveillantes.



2- LES MENACES

- Ce sont des causes potentielles d'incident, déterminés capables de monter une attaque exploitant une vulnérabilité.
- Ex: Un logiciel espion, un courrier indésirable.



3- LES ATTAQUES

- Elles représentent les moyens d'exploiter une vulnérabilité.
- Il peut y avoir plusieurs attaques pour une même vulnérabilité.



V- LES MENACES LES PLUS COURANTES

1- Virus informatique

- Un virus informatique est un type de logiciel malveillant caché dans un logiciel légitime développé par un Hacker.
- Chaque fois qu’un utilisateur ouvre le logiciel infecté, il permet au virus de se propager. Il perturbe plus ou moins gravement le fonctionnement de l'ordinateur infecté.
- Il peut se répandre par tout moyen d’échange de données numériques comme les réseaux informatiques et les clefs USB.



Solution:

- Logiciels Anti-Virus.

V- LES MENACES LES PLUS COURANTES

2- Ver informatique (Computer Worm):

- Le virus ne doit pas être confondu avec un ver informatique, qui se répand sur le réseau Internet. Ce dernier peut s’installer sur un ordinateur à partir d’un courriel, par téléchargement d’un fichier ou par messagerie instantanée.
- On appelle ces courriels des Pourriels (Spam)
- Les vers installent généralement sur l'ordinateur des Logiciels malveillants (Malware).



Solution:

- Il faut toujours mettre à jour votre système et les programmes régulièrement.

V- LES MENACES LES PLUS COURANTES

3- Logiciel malveillant (Malware):

- Un logiciel malveillant peut corrompre, effacer ou voler les données des appareils informatiques.

Exemples:

- Logiciel espion (Spyware), Cheval de Troie (Trojan horse), Keylogger: Tous ces programmes peuvent être exploités pour espionner votre activité, capturer des mots de passe ou numéros de carte bancaire, ou prendre le contrôle de l'ordinateur à distance.

Solution:

- Logiciels Anti-Malware.





V- LES MENACES LES PLUS COURANTES

4- Hameçonnage (Phishing):

- La fraude par hameçonnage est une des menaces informatiques les plus facile à identifier. Il s’agit d’un courriel qui ressemble à s’y méprendre à celui d’un service connu, comme une institution bancaire.
- Le fraudeur tente d’obtenir des informations personnelles en incitant l’utilisateur à cliquer sur un lien, par exemple pour vérifier l’identification d’un compte de carte de crédit.
- Les banques le répètent pourtant : jamais elles ne demandent de renseignements personnels à leurs clients de cette manière.

« 76 % DES ENTREPRISES ONT ÉTÉ VICTIMES D’UNE ATTAQUE PAR PHISHING EN 2017 »

- Wombat security



VI- PIRATES (HACKERS)

- Les pirates ne sont pas mauvais en soi – le mot «Hacker» ne signifie pas «criminel». Les rédacteurs font souvent référence à trois types de hackers : « Black Hat | chapeau noir », « White Hat | chapeau blanc » et «Grey Hat | chapeau gris » . Ces termes définissent les différents groupes de pirates en se basant sur leur comportement.

- La définition du mot «Hacker» est controversée, il peut signifier soit quelqu'un qui compromet la sécurité des ordinateurs soit d'un développeur qualifié dans les logiciels.



Black Hackers



Ils traitent souvent des sujet comme le viol de la sécurité des ordinateurs à des fins profitants à celui-ci (vol de numéros de carte de crédit, récoltes de données personnelles pour vente massive…)

Grey Hackers



Il pourrait compromis un système informatique sans autorisation, et n'informer l'organisation qu'après l'avoir fait, leur permettant ainsi de résoudre le problème.

White Hackers



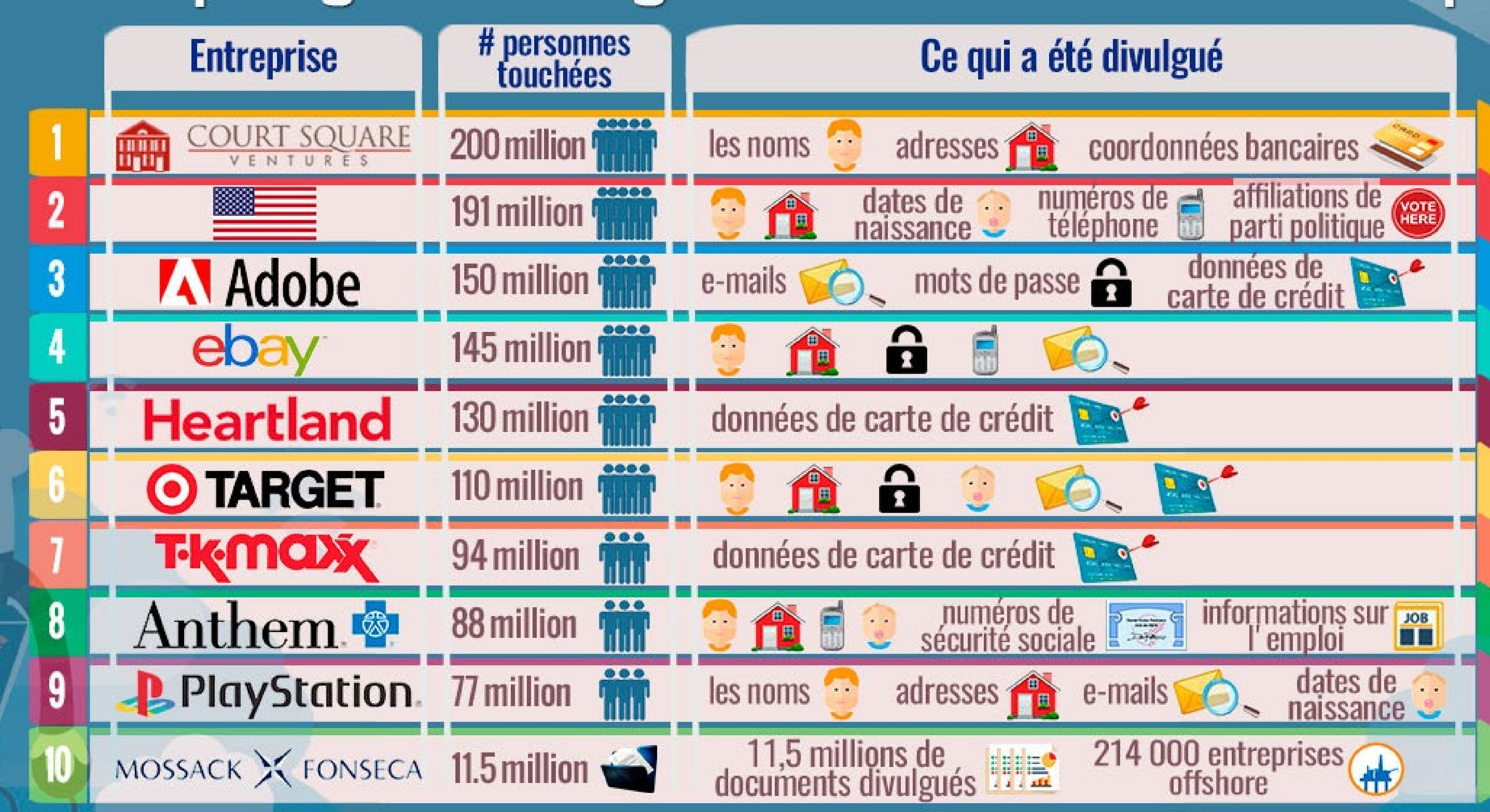
Ils sont les « hackers éthiques » , des experts en sécurité informatique qui utilisent leurs capacités à des fins honnêtes , éthiques et du côté de la justice plutôt que des fins malhonnêtes, contraires à la loi, pour profit… Ils sont embauchés pour tester les systèmes de sécurité informatique d'une organisation.

Autres types des Hackers

Les Hacktivistes : un ensemble de « hacker » et « activiste », ils agissent pour défendre une cause souvent politique.

Les script-kiddies : les gamins qui utilisent les scripts loin d'avoir compris les principaux principes et éthiques d'un hacker, ils utilisent des scripts et programmes tout fait (par des vrai Hackers) pour endommager et causer des pertes…

VII- ÉTUDES DES CAS



VIII- CONSEILS POUR PROTÉGER VOTRE ORDINATEUR

1. Utiliser un mot de passe rigoureuse.
2. Utilisez des applications anti-malware et anti-virus.
3. Maintenez Windows et vos applications à jour.
4. N'ouvrez pas les messages électroniques provenant d'expéditeurs inconnus ou les pièces jointes que vous ne reconnaissez pas.
5. Effacez votre cache Internet et votre historique de navigation.
6. Utilisez un pare-feu.

